Into the rabbit hole: Computing HD isogenies through graph theory

Max Duparc

EPFL
LASEC

KULB-seminars: March 27, 2026

Current state of isogenies

- HD isogenies are everywhere:
  - dim 2: SQIsign (& var.), PRISM, POKE (& var.), DeuringVRF, ...
  - dim 4: SQIsignHD, (qt-)Pegasis, $\otimes$-MIKE, ...
  - dim 8: Attacks

Current state of isogenies

- HD isogenies are everywhere:
  - dim 2: SQIsign (& var.), PRISM, POKE (& var.), DeuringVRF, ...
  - dim 4: SQIsignHD, (qt-)Pegasis, $\otimes$-MIKE, ...
  - dim 8: Attacks
- Computing HD isogenies is scary !
  - Hard maths $\cap$ Technical programming.

Current state of isogenies

- HD isogenies are everywhere:
  - dim 2: SQIsign (& var.), PRISM, POKE (& var.), DeuringVRF, ...
  - dim 4: SQIsignHD, (qt-)Pegasis, $\otimes$-MIKE, ...
  - dim 8: Attacks
- Computing HD isogenies is scary !
  - Hard maths $\cap$ Technical programming.

  $=$ Its a rabbit-hole.

Current state of isogenies

- HD isogenies are everywhere:
  - dim 2: SQIsign (& var.), PRISM, POKE (& var.), DeuringVRF, ...
  - dim 4: SQIsignHD, (qt-)Pegasis, $\otimes$-MIKE, ...
  - dim 8: Attacks
- Computing HD isogenies is scary !
  - Hard maths $\cap$ Technical programming.

  $=$ Its a rabbit-hole.

- Big limiting factor of isogeny based cryptography in near futur !

History rhymes

"The security of cryptosystems based on elliptic curves is not well understood, due in large part to the abstruse nature of elliptic curves. Few cryptographers understand elliptic curves [...] Over time, this may change, but for now trying to get an evaluation of the security of an elliptic-curve cryptosystem is a bit like trying to get an evaluation of some recently discovered Chaldean poetry."

— Ron Rivest (mid-1990s)

History rhymes

"The security of cryptosystems based on elliptic curves is not well understood, due in large part to the abstruse nature of elliptic curves. Few cryptographers understand elliptic curves [...] Over time, this may change, but for now trying to get an evaluation of the security of an elliptic-curve cryptosystem is a bit like trying to get an evaluation of some recently discovered Chaldean poetry."

— Ron Rivest (mid-1990s)

Today's program

1. Introduce simplified theory to HD isogenies[a] !

[a] Focus on 2-isogenies.

History rhymes

"The security of cryptosystems based on elliptic curves is not well understood, due in large part to the abstruse nature of elliptic curves. Few cryptographers understand elliptic curves [...] Over time, this may change, but for now trying to get an evaluation of the security of an elliptic-curve cryptosystem is a bit like trying to get an evaluation of some recently discovered Chaldean poetry."

— Ron Rivest (mid-1990s)

Today's program

1. Introduce simplified theory to HD isogenies[a] !
2. Use it to gain speed-up and flexibility !

[a] Focus on 2-isogenies.

History rhymes

"The security of cryptosystems based on elliptic curves is not well understood, due in large part to the abstruse nature of elliptic curves. Few cryptographers understand elliptic curves [...] Over time, this may change, but for now trying to get an evaluation of the security of an elliptic-curve cryptosystem is a bit like trying to get an evaluation of some recently discovered Chaldean poetry."

— Ron Rivest (mid-1990s)

Today's program

1. Introduce simplified theory to HD isogenies[a] !
2. Use it to gain speed-up and flexibility !
3. Explore the rabbit hole of new possibilities.

[a] Focus on 2-isogenies.

On the shoulders of giants

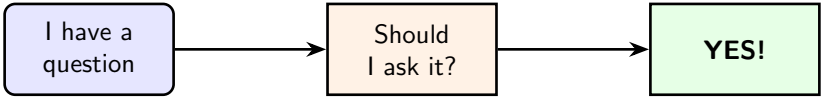
Talk based on the following works:

- [Dup25] *Superglue: Fast formulae for (2,2)-gluing isogenies*, single author, ASIACRYPT 2025.
- [DD26] *Chasing Rabbits Through Hypercubes: Better algorithms for higher dimensional 2-isogeny computations*, with Pierrick Dartois, preprint, 2026.
- $\otimes$*-MIKE for mere mortals (working title)*, with the MIKE-team *(in preparation)*.

Part is a palimpsest of the following work:

- [Dar25] *Fast computation of higher dimensional isogenies for cryptographic applications*, by Pierrick Dartois, PhD Thesis, 2025

This is an IOP



Always remember [Sha92]

$$\mathsf{IP} = \mathsf{PSPACE}$$

Table of Contents

Abelian varieties

$$E$$

- Abelian varieties of dim 1.
- $E[N] \cong \mathbb{Z}_N^2$

Abelian varieties

$$(E, e^E)$$

- Abelian varieties of dim 1.
- $E[N] \cong \mathbb{Z}_N^2$
- Alternating compatible non-degenerate pairing

$$\forall N \in \mathbb{N}, \quad e_N^E : E[N] \times E[N] \longrightarrow \mu_N$$

Abelian varieties

(E, e^E)

- Abelian varieties of dim 1.
- $E[N] \cong \mathbb{Z}_N^2$
- Alternating compatible non-degenerate pairing

$$\forall N \in \mathbb{N}, \quad e_N^E : E[N] \times E[N] \longrightarrow \mu_N$$

(A, e^A)

- Abelian varieties of dim g.
- $A[N] \cong \mathbb{Z}_N^{2g}$
- Alternating compatible non-degenerate pairing

$$\forall N \in \mathbb{N}, \quad e_N^A : A[N] \times A[N] \longrightarrow \mu_N$$

Abelian varieties

(E, e^E)

- Abelian varieties of dim 1.
- $E[N] \cong \mathbb{Z}_N^2$
- Alternating compatible non-degenerate pairing

$$\forall N \in \mathbb{N}, \quad e_N^E : E[N] \times E[N] \longrightarrow \mu_N$$

(A, e^A)

- Abelian varieties of dim g.
- $A[N] \cong \mathbb{Z}_N^{2g}$
- Alternating compatible non-degenerate pairing

$$\forall N \in \mathbb{N}, \quad e_N^A : A[N] \times A[N] \longrightarrow \mu_N$$

Isogenies

$$f : (E, e^E) \longrightarrow (\overline{E}, e^{\overline{E}})$$

- Surjective morphism $\implies |\ker(f)| < \infty$.
- Compatible with group structures.
- $\ker(f)$ cyclic.

Abelian varieties

(E, e^E)

- Abelian varieties of dim 1.
- $E[N] \cong \mathbb{Z}_N^2$
- Alternating compatible non-degenerate pairing

$$\forall N \in \mathbb{N}, \quad e_N^E : E[N] \times E[N] \longrightarrow \mu_N$$

(A, e^A)

- Abelian varieties of dim g.
- $A[N] \cong \mathbb{Z}_N^{2g}$
- Alternating compatible non-degenerate pairing

$$\forall N \in \mathbb{N}, \quad e_N^A : A[N] \times A[N] \longrightarrow \mu_N$$

Isogenies

$$f : (E, e^E) \longrightarrow (\overline{E}, e^{\overline{E}})$$

- Surjective morphism $\implies |\ker(f)| < \infty$.
- Compatible with group structures.
- $\ker(f)$ cyclic.

- $e^E\big(f(P), f(Q)\big) = e^{\overline{E}}(P, Q)^{\deg(f)}$
- dual $\widetilde{f} : (\overline{E}, e^{\overline{E}}) \to (E, e^E)$ with $\ker(\widetilde{f}) = f\,(E[\deg(f)])$.

Abelian varieties

(E, e^E)

- Abelian varieties of dim 1.
- $E[N] \cong \mathbb{Z}_N^2$
- Alternating compatible non-degenerate pairing

$$\forall N \in \mathbb{N}, \quad e_N^E : E[N] \times E[N] \longrightarrow \mu_N$$

(A, e^A)

- Abelian varieties of dim g.
- $A[N] \cong \mathbb{Z}_N^{2g}$
- Alternating compatible non-degenerate pairing

$$\forall N \in \mathbb{N}, \quad e_N^A : A[N] \times A[N] \longrightarrow \mu_N$$

Isogenies

$$f : (A, e^A) \longrightarrow (B, e^B)$$

- Surjective morphism $\implies |\ker(f)| < \infty$.
- Compatible with group structures.
- $\ker(f)$ max. isotropic ($e^A|_{\ker(f)^2} \equiv 1$).

- $e^B\big(f(P), f(Q)\big) = e^A(P, Q)^{\deg(f)}$
- dual $\widetilde{f} : (B, e^B) \to (A, e^A)$ with $\ker(\widetilde{f}) = f\,(A[\deg(f)])$.

Symplectic form

Need representation of $A[N] \cong \mathbb{Z}_N^{2g}$ compatible with e^A

Symplectic form

Need representation of $A[N] \cong \mathbb{Z}_N^{2g}$ compatible with e^A

Symplectic representation

- Using $\widehat{\mathbb{Z}_N^g} = \{\chi : \mathbb{Z}_N^g \longrightarrow \mu_N\}$ the dual of $\mathbb{Z}_N^g$[a], let:

$$\epsilon : \left(\mathbb{Z}_N^g \times \widehat{\mathbb{Z}_N^g}\right)^2 \longrightarrow \mu_N, \quad \text{s.t.} \quad \epsilon\big((x_1,\chi_1),(x_2,\chi_2)\big) = \chi_2(x_1)\cdot\chi_1(x_2)^{-1}$$

[a] $\chi_i(-) \rightsquigarrow \zeta^{\langle x_i|-\rangle}$ for ζ a primitive N-root of unity and $x_i \in \mathbb{Z}_N^g$.

Symplectic form

Need representation of $A[N] \cong \mathbb{Z}_N^{2g}$ compatible with e^A

Symplectic representation

- Using $\widehat{\mathbb{Z}_N^g} = \{\chi : \mathbb{Z}_N^g \longrightarrow \mu_N\}$ the dual of $\mathbb{Z}_N^g$[a], let:

$$\epsilon : \left(\mathbb{Z}_N^g \times \widehat{\mathbb{Z}_N^g}\right)^2 \longrightarrow \mu_N, \quad \text{s.t.} \quad \epsilon\big((x_1,\chi_1),(x_2,\chi_2)\big) = \chi_2(x_1)\cdot\chi_1(x_2)^{-1}$$

- **Symplectic representation** of $A[N]$:

$$\mu : (A[N], e_A) \xrightarrow{\cong} (\mathbb{Z}_N^g \times \widehat{\mathbb{Z}_N^g}, \epsilon)$$

[a] $\chi_i(-) \rightsquigarrow \zeta^{\langle x_i|-\rangle}$ for ζ a primitive N-root of unity and $x_i \in \mathbb{Z}_N^g$.

Symplectic form

Need representation of $A[N] \cong \mathbb{Z}_N^{2g}$ compatible with e^A

Symplectic representation

- Using $\widehat{\mathbb{Z}_N^g} = \{\chi : \mathbb{Z}_N^g \longrightarrow \mu_N\}$ the dual of $\mathbb{Z}_N^g$[a], let:

$$\epsilon : \left(\mathbb{Z}_N^g \times \widehat{\mathbb{Z}_N^g}\right)^2 \longrightarrow \mu_N, \quad \text{s.t.} \quad \epsilon\big((x_1,\chi_1),(x_2,\chi_2)\big) = \chi_2(x_1)\cdot\chi_1(x_2)^{-1}$$

- **Symplectic representation** of $A[N]$:

$$\mu : (A[N], e_A) \xrightarrow{\cong} (\mathbb{Z}_N^g \times \widehat{\mathbb{Z}_N^g}, \epsilon)$$

- Equivalent to **symplectic basis** $\mathcal{B}_\mu := \{S_1, \dots, S_g, T_1, \dots, T_g\}$:

$$e_A(S_i, S_j) = e_A(T_i, T_j) = 1, \quad e_A(S_i, T_j) = \zeta^{\delta_{i,j}}$$

[a] $\chi_i(-) \leftrightsquigarrow \zeta^{\langle x_i|-\rangle}$ for ζ a primitive N-root of unity and $x_i \in \mathbb{Z}_N^g$.

Theta structures

Definition

1. A symplectic representation $\mu_A : A[N] \xrightarrow{\cong} \mathbb{Z}_N^g \times \widehat{\mathbb{Z}_N^g}$;

Theta structures

Definition

1. A symplectic representation $\mu_A : A[N] \xrightarrow{\cong} \mathbb{Z}_N^g \times \widehat{\mathbb{Z}_N^g}$;
2. A map

$$\begin{array}{rcl} \theta^A : A & \longrightarrow & \mathbb{P}_k^{N^g-1} \\ \theta^A(P) & \longrightarrow & \left(\theta_i^A(P)\right)_{i \in \mathbb{Z}_N^g} \end{array}$$

Theta structures

Definition

1. A symplectic representation $\mu_A : A[N] \xrightarrow{\cong} \mathbb{Z}_N^g \times \widehat{\mathbb{Z}_N^g}$;
2. A map

$$\begin{array}{rcl} \theta^A : A & \longrightarrow & \mathbb{P}_k^{N^g-1} \\ \theta^A(P) & \longrightarrow & \left(\theta_i^A(P)\right)_{i\in\mathbb{Z}_N^g} \end{array}$$

satisfying the *theta group action relation*:

$$\forall P \in A, Q \in A[N] \text{ with } \mu_A(Q) = (x_Q, \chi_Q) : \quad \theta_j^A(P+Q) = \chi_Q(j)^{-1}\theta_{j+x_Q}^A(P)$$

Theta structures

Definition

1. A symplectic representation $\mu_A : A[N] \xrightarrow{\cong} \mathbb{Z}_N^g \times \widehat{\mathbb{Z}_N^g}$;
2. A map

$$\begin{array}{rcl} \theta^A : A & \longrightarrow & \mathbb{P}_k^{N^g-1} \\ \theta^A(P) & \longrightarrow & \left(\theta_i^A(P)\right)_{i\in\mathbb{Z}_N^g} \end{array}$$

satisfying the *theta group action relation*:

$$\forall P \in A, Q \in A[N] \text{ with } \mu_A(Q) = (x_Q, \chi_Q) : \quad \theta_j^A(P+Q) = \chi_Q(j)^{-1}\theta_{j+x_Q}^A(P)$$

- We are interested in symmetric theta structure with $N = 2$:
  - Optimal for computation.
  - $\theta^A(0)$ characterises A (up to isomorphism).
  - It is *symmetric*: (i.e. $\theta^A(-P) = \theta^A(P)$).

Theta structures

Definition

1. A symplectic representation $\mu_A : A[N] \xrightarrow{\cong} \mathbb{Z}_N^g \times \widehat{\mathbb{Z}_N^g}$;
2. A map

$$\begin{array}{rcl} \theta^A : A & \longrightarrow & \mathbb{P}_k^{N^g-1} \\ \theta^A(P) & \longrightarrow & \left(\theta_i^A(P)\right)_{i\in\mathbb{Z}_N^g} \end{array}$$

satisfying the *theta group action relation*:

$$\forall P \in A, Q \in A[N] \text{ with } \mu_A(Q) = (x_Q, \chi_Q) : \quad \theta_j^A(P+Q) = \chi_Q(j)^{-1}\theta_{j+x_Q}^A(P)$$

- We are interested in symmetric theta structure with $N = 2$:
  - Optimal for computation.
  - $\theta^A(0)$ characterises A (up to isomorphism).
  - It is *symmetric*: (i.e. $\theta^A(-P) = \theta^A(P)$).
- How do we construct a theta structure ?

Constructing theta structures

Theta structures are linear algebra !

Constructing theta structures

Theta structures are linear algebra !

$$\theta^A : A \longrightarrow \mathbb{P}^{2^g-1} \quad \rightsquigarrow \quad \Theta^A \in \mathrm{PGL}_{2^g}$$

Constructing theta structures

Theta structures are linear algebra !

$$\theta^A : A \longrightarrow \mathbb{P}^{2^g-1} \quad \leftrightsquigarrow \quad \Theta^A \in \mathrm{PGL}_{2^g}$$

- Let $\mu_A \leftrightsquigarrow \{S_1, \cdots, S_g, T_1, \cdots, T_g\}$
  Theta structure are linear combinations of *translation maps* $\mathfrak{t}_{S_i}$ and $\mathfrak{t}_{T_i}$:

Constructing theta structures

Theta structures are linear algebra !

$$\theta^A : A \longrightarrow \mathbb{P}^{2^g-1} \quad \rightsquigarrow \quad \Theta^A \in \mathrm{PGL}_{2^g}$$

- Let $\mu_A \rightsquigarrow \{S_1, \cdots, S_g, T_1, \cdots, T_g\}$
  Theta structure are linear combinations of *translation maps* $\mathfrak{t}_{S_i}$ and $\mathfrak{t}_{T_i}$:

Row-wise:
$$\begin{cases} \Theta_i \cdot \mathfrak{t}_{T_1} &= (-1)^{\langle 01|i\rangle} \cdot \Theta_i \\ \Theta_i \cdot \mathfrak{t}_{T_2} &= (-1)^{\langle 10|i\rangle} \cdot \Theta_i \\ \Theta_i \cdot \mathfrak{t}_{S_1} &= \Theta_{i+01} \\ \Theta_i \cdot \mathfrak{t}_{S_2} &= \Theta_{i+10} \end{cases}$$

Constructing theta structures

Theta structures are linear algebra !

$$\theta^A : A \longrightarrow \mathbb{P}^{2^g-1} \quad \leftrightsquigarrow \quad \Theta^A \in \mathrm{PGL}_{2^g}$$

- Let $\mu_A \leftrightsquigarrow \{S_1, \cdots, S_g, T_1, \cdots, T_g\}$
  Theta structure are linear combinations of *translation maps* $\mathfrak{t}_{S_i}$ and $\mathfrak{t}_{T_i}$:

$$\text{Row-wise: } \begin{cases} \Theta_i \cdot \mathfrak{t}_{T_1} &= (-1)^{\langle 01|i\rangle} \cdot \Theta_i \\ \Theta_i \cdot \mathfrak{t}_{T_2} &= (-1)^{\langle 10|i\rangle} \cdot \Theta_i \\ \Theta_i \cdot \mathfrak{t}_{S_1} &= \Theta_{i+01} \\ \Theta_i \cdot \mathfrak{t}_{S_2} &= \Theta_{i+10} \end{cases} \implies \begin{cases} \Theta_{00} &= \left[\mathfrak{t}_0 + \mathfrak{t}_{T_1} + \mathfrak{t}_{T_2} + \mathfrak{t}_{T_1+T_2}\right]_{0,*} \\ \Theta_{01} &= \Theta_{00} \cdot \mathfrak{t}_{S_1} \\ \Theta_{10} &= \Theta_{00} \cdot \mathfrak{t}_{S_2} \\ \Theta_{11} &= \Theta_{00} \cdot \mathfrak{t}_{S_1+S_2} \end{cases}$$

Constructing theta structures

Theta structures are linear algebra !

$$\theta^A : A \longrightarrow \mathbb{P}^{2^g-1} \quad \rightsquigarrow \quad \Theta^A \in \mathrm{PGL}_{2^g}$$

- Let $\mu_A \rightsquigarrow \{S_1, \cdots, S_g, T_1, \cdots, T_g\}$
  Theta structure are linear combinations of *translation maps* $\mathfrak{t}_{S_i}$ and $\mathfrak{t}_{T_i}$:

$$\text{Row-wise: } \begin{cases} \Theta_i \cdot \mathfrak{t}_{T_1} &= (-1)^{\langle 01|i\rangle} \cdot \Theta_i \\ \Theta_i \cdot \mathfrak{t}_{T_2} &= (-1)^{\langle 10|i\rangle} \cdot \Theta_i \\ \Theta_i \cdot \mathfrak{t}_{S_1} &= \Theta_{i+01} \\ \Theta_i \cdot \mathfrak{t}_{S_2} &= \Theta_{i+10} \end{cases} \implies \begin{cases} \Theta_{00} &= \left[\mathfrak{t}_0 + \mathfrak{t}_{T_1} + \mathfrak{t}_{T_2} + \mathfrak{t}_{T_1+T_2}\right]_{0,*} \\ \Theta_{01} &= \Theta_{00} \cdot \mathfrak{t}_{S_1} \\ \Theta_{10} &= \Theta_{00} \cdot \mathfrak{t}_{S_2} \\ \Theta_{11} &= \Theta_{00} \cdot \mathfrak{t}_{S_1+S_2} \end{cases}$$

Question: Can you spot the problem ?

Constructing theta structures

Theta structures are linear algebra !

$$\theta^A : A \longrightarrow \mathbb{P}^{2^g-1} \quad \rightsquigarrow \quad \Theta^A \in \mathrm{PGL}_{2^g}$$

- Let $\mu_A \rightsquigarrow \{S_1, \cdots, S_g, T_1, \cdots, T_g\}$
  Theta structure are linear combinations of *translation maps* $\mathfrak{t}_{S_i}$ and $\mathfrak{t}_{T_i}$:

$$\text{Row-wise: } \begin{cases} \Theta_i \cdot \mathfrak{t}_{T_1} &= (-1)^{\langle 01|i\rangle} \cdot \Theta_i \\ \Theta_i \cdot \mathfrak{t}_{T_2} &= (-1)^{\langle 10|i\rangle} \cdot \Theta_i \\ \Theta_i \cdot \mathfrak{t}_{S_1} &= \Theta_{i+01} \\ \Theta_i \cdot \mathfrak{t}_{S_2} &= \Theta_{i+10} \end{cases} \implies \begin{cases} \Theta_{00} &= \left[\mathfrak{t}_0 + \mathfrak{t}_{T_1} + \mathfrak{t}_{T_2} + \mathfrak{t}_{T_1+T_2}\right]_{0,*} \\ \Theta_{01} &= \Theta_{00} \cdot \mathfrak{t}_{S_1} \\ \Theta_{10} &= \Theta_{00} \cdot \mathfrak{t}_{S_2} \\ \Theta_{11} &= \Theta_{00} \cdot \mathfrak{t}_{S_1+S_2} \end{cases}$$

Question: Can you spot the problem ?

- $\mathfrak{t}_{T_j}$ are projective, so addition is not well defined !

Consistant translation maps

1. Ensure that $\mathfrak{t}_P$ are involutions. (i.e. $\det(\mathfrak{t}_P) = \pm 1$).

Consistant translation maps

1. Ensure that $\mathfrak{t}_P$ are involutions. (i.e. $\det(\mathfrak{t}_P) = \pm 1$).
   - But, still have sign ambiguity !

Consistant translation maps

1. Ensure that $\mathfrak{t}_P$ are involutions. (i.e. $\det(\mathfrak{t}_P) = \pm 1$).
   - But, still have sign ambiguity !

2. Solve the sign ambiguity using *symmetric elements*:

Consistant translation maps

1. Ensure that $\mathfrak{t}_P$ are involutions. (i.e. $\det(\mathfrak{t}_P) = \pm 1$).
   - But, still have sign ambiguity !

2. Solve the sign ambiguity using *symmetric elements*:
   - Let $A[4] = \{S_1', \cdots, S_g', T_1', \cdots, T_g'\}$.

     $$\mathfrak{g}_{X_i'} := \pm \mathfrak{t}_{X_i}$$

     such that X_i' is in the eigenspace of 1.

Consistant translation maps

1. Ensure that $\mathfrak{t}_P$ are involutions. (i.e. $\det(\mathfrak{t}_P) = \pm 1$).
   - But, still have sign ambiguity !

2. Solve the sign ambiguity using *symmetric elements*:
   - Let $A[4] = \{S_1', \cdots, S_g', T_1', \cdots, T_g'\}$.

     $$\mathfrak{g}_{X_i'} := \pm \mathfrak{t}_{X_i}$$

     such that X_i' is in the eigenspace of 1.

   - Remaining $\mathfrak{g}_X$ for $X \in A[4]$ computable using pairing e^A.

     $$\mathfrak{g}_P \cdot \mathfrak{g}_Q = e_4^A(P, Q) \cdot \mathfrak{g}_{P+Q}$$

Consistant translation maps

1. Ensure that $\mathfrak{t}_P$ are involutions. (i.e. $\det(\mathfrak{t}_P) = \pm 1$).
   - But, still have sign ambiguity !

2. Solve the sign ambiguity using *symmetric elements*:
   - Let $A[4] = \{S'_1, \cdots, S'_g, T'_1, \cdots, T'_g\}$.

     $$\mathfrak{g}_{X'_i} := \pm \mathfrak{t}_{X_i}$$

     such that X'_i is in the eigenspace of 1.
   - Remaining $\mathfrak{g}_X$ for $X \in A[4]$ computable using pairing e^A.

     $$\mathfrak{g}_P \cdot \mathfrak{g}_Q = e_4^A(P, Q) \cdot \mathfrak{g}_{P+Q}$$

[Mum66] Mumford theorem (simplified)

Symplectic basis of $A[4] \implies \Theta^A$ theta structures (of level 2)

Example: Montgomery curves

- On Kummer line $E_{/\pm 1}$:

  $\mathfrak{g}_P \cdot \mathfrak{g}_Q = \pm \mathbf{i}\mathfrak{g}_{P+Q} = -\mathfrak{g}_Q \cdot \mathfrak{g}_P$

[1] $u = a^2 + b^2$, $v = a^2 - b^2$

Example: Montgomery curves

- On Kummer line $E_{/\pm 1}$:

  $\mathfrak{g}_P \cdot \mathfrak{g}_Q = \pm \mathbf{i} \mathfrak{g}_{P+Q} = -\mathfrak{g}_Q \cdot \mathfrak{g}_P$

- $\simeq X, Y, Z$ Pauli matrices.

Pauli Matrices

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad Y = \begin{pmatrix} 0 & -\mathbf{i} \\ \mathbf{i} & 0 \end{pmatrix} \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Example: Montgomery curves

- On Kummer line $E_{/\pm 1}$:

  $\mathfrak{g}_P \cdot \mathfrak{g}_Q = \pm \mathbf{i}\mathfrak{g}_{P+Q} = -\mathfrak{g}_Q \cdot \mathfrak{g}_P$

- $\simeq X, Y, Z$ Pauli matrices.

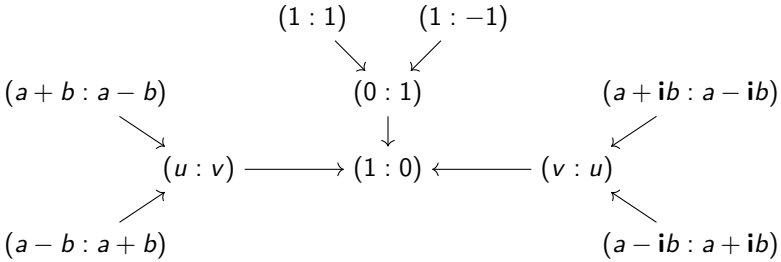


Figure: Structure of $E[4]_{/\pm 1}$ on Montgomery curves[1]

Pauli Matrices

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad Y = \begin{pmatrix} 0 & -\mathbf{i} \\ \mathbf{i} & 0 \end{pmatrix} \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Example: Montgomery curves

- On Kummer line $E_{/\pm 1}$:

  $\mathfrak{g}_P \cdot \mathfrak{g}_Q = \pm \mathbf{i} \mathfrak{g}_{P+Q} = -\mathfrak{g}_Q \cdot \mathfrak{g}_P$

- $\simeq X, Y, Z$ Pauli matrices.

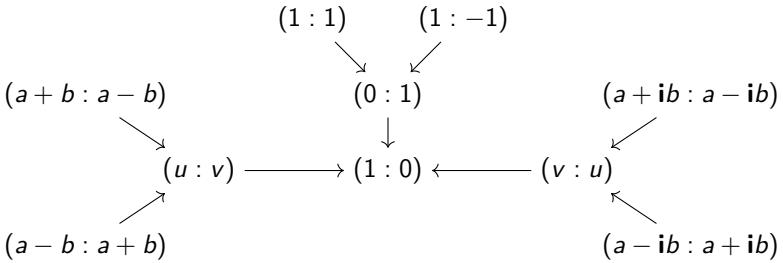


Figure: Structure of $E[4]_{/\pm 1}$ on Montgomery curves[1]

Symmetric elements on Montgomery curves

$$\mathfrak{g}_{(1:\pm 1)} = \pm X \qquad \mathfrak{g}_{(a\pm b:a\mp b)} = \pm \frac{1}{2ab}\left(uZ - \mathbf{i}vY\right) \qquad \mathfrak{g}_{(a\pm \mathbf{i}b:a\mp \mathbf{i}b)} = \mp \frac{1}{2ab}\left(\mathbf{i}vZ + uY\right)$$

[1] $u = a^2 + b^2$, $v = a^2 - b^2$

Example: Theta model

Translation in the theta model

$$\mathfrak{g}_P \iff \text{theta action over } \Theta^A$$

Example: Theta model

Translation in the theta model

$$\mathfrak{g}_P \iff \text{theta action over } \Theta^A$$

$$\mathfrak{g}_{S_1} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \qquad \mathfrak{g}_{S_2} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

$$\mathfrak{g}_{T_1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}, \quad \mathfrak{g}_{T_2} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

Example: Theta model

Translation in the theta model

$$\mathfrak{g}_P \iff \text{theta action over } \Theta^A$$

$$\mathfrak{g}_{S_1} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \qquad \mathfrak{g}_{S_2} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

$$\mathfrak{g}_{T_1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}, \quad \mathfrak{g}_{T_2} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

Theta model $\iff$ Fixing canonical form of $\mathfrak{g}_P$

Duality on theta structures

Duality on theta structures

$$A[4] = \{S_1, \dots, S_g, T_1, \dots, T_g\}$$

$$A[4] = \{T_1, \dots, T_g, -S_1, \dots, -S_g\}$$

Duality on theta structures

$$A[4] = \{S_1, \dots, S_g, T_1, \dots, T_g\} \quad \xleftrightarrow{\begin{pmatrix} 0 & -I_g \\ I_g & 0 \end{pmatrix}} \quad A[4] = \{T_1, \dots, T_g, -S_1, \dots, -S_g\}$$

Duality on theta structures

$$A[4] = \{S_1, \dots, S_g, T_1, \dots, T_g\} \qquad \xleftrightarrow{\begin{pmatrix} 0 & -I_g \\ I_g & 0 \end{pmatrix}} \qquad A[4] = \{T_1, \dots, T_g, -S_1, \dots, -S_g\}$$

$$\Downarrow \qquad\qquad\qquad\qquad\qquad\qquad \Downarrow$$

$$\theta^A : A \longrightarrow \mathbb{P}^{2^{g-1}} \qquad\qquad \widetilde{\theta}^A : A \longrightarrow \mathbb{P}^{2^{g-1}}$$

Duality on theta structures

$$A[4] = \{S_1, \dots, S_g, T_1, \dots, T_g\} \quad \xleftrightarrow{\begin{pmatrix} 0 & -I_g \\ I_g & 0 \end{pmatrix}} \quad A[4] = \{T_1, \dots, T_g, -S_1, \dots, -S_g\}$$

$$\Downarrow \qquad\qquad\qquad\qquad \Downarrow$$

$$\theta^A : A \longrightarrow \mathbb{P}^{2^{g-1}} \quad \xleftrightarrow{\mathcal{H}} \quad \widetilde{\theta}^A : A \longrightarrow \mathbb{P}^{2^{g-1}}$$

$$\mathcal{H} : (x_i)_{i \in \mathbb{Z}_2^g} \longrightarrow \left(\sum_{i \in \mathbb{Z}_2^g} (-1)^{\langle j | i \rangle} x_i \right)_{j \in \mathbb{Z}_2^g}$$

Duality on theta structures

$$A[4] = \{S_1, \dots, S_g, T_1, \dots, T_g\} \quad \xleftrightarrow{\begin{pmatrix} 0 & -I_g \\ I_g & 0 \end{pmatrix}} \quad A[4] = \{T_1, \dots, T_g, -S_1, \dots, -S_g\}$$

$$\Downarrow \qquad\qquad\qquad\qquad \Downarrow$$

$$\theta^A : A \longrightarrow \mathbb{P}^{2^{g-1}} \quad \xleftrightarrow{\mathcal{H}} \quad \widetilde{\theta}^A : A \longrightarrow \mathbb{P}^{2^{g-1}}$$

$$\mathcal{H} : (x_i)_{i \in \mathbb{Z}_2^g} \longrightarrow \left(\sum_{i \in \mathbb{Z}_2^g} (-1)^{\langle j | i \rangle} x_i \right)_{j \in \mathbb{Z}_2^g}$$

Notation:

$$(x_i)_i \odot (y_i)_i = (x_i y_i)_i \qquad (x_i)_i^{\odot n} = (x_i^n)_i \text{ for } n \in \mathbb{Z}.$$

Isogeny Formula

$$(A, e_A) \xrightarrow{f \text{ of degree } 2} (B, e_B)$$

Isogeny Formula

$$(A, e_A) \xrightarrow{f \text{ of degree } 2} (B, e_B)$$

$$A[8] = \langle S_1, \cdots, S_g, T_1, \cdots, T_g \rangle \xrightarrow{\ker(f)=[4]K_T}$$

$$A[4] = [2](K_S \oplus K_T) \xleftarrow{\ker(\widehat{f})=[4]f(K_S)} B[4] = [2]f(K_S) \oplus f(K_T)$$

Isogeny Formula

$$(A, e_A) \xrightarrow{f \text{ of degree } 2} (B, e_B)$$

$$A[8] = \langle S_1, \cdots, S_g, T_1, \cdots, T_g \rangle \xrightarrow{\ker(f)=[4]K_T} B[4] = [2]f(K_S) \oplus f(K_T)$$

$$A[4] = [2](K_S \oplus K_T) \xleftarrow{\ker(\widehat{f})=[4]f(K_S)}$$

$$\theta^A : A \longrightarrow \mathbb{P}^{2^g-1} \qquad \theta^B : B \longrightarrow \mathbb{P}^{2^g-1}$$

Isogeny Formula

$$(A, e_A) \xrightarrow{f \text{ of degree } 2} (B, e_B)$$

$$A[8] = \langle S_1, \cdots, S_g, T_1, \cdots, T_g \rangle \xrightarrow{\ker(f)=[4]K_T} B[4] = [2]f(K_S) \oplus f(K_T)$$

$$A[4] = [2](K_S \oplus K_T) \xleftarrow{\ker(\widehat{f})=[4]f(K_S)}$$

$$\theta^A : A \longrightarrow \mathbb{P}^{2^{g-1}} \xrightarrow{\text{Isogeny formula}} \theta^B : B \longrightarrow \mathbb{P}^{2^{g-1}}$$

Isogeny Formula

$$\mathcal{H}\left(\theta^A(P+Q) \odot \theta^A(P-Q)\right) = \widetilde{\theta}^B(f(P)) \odot \widetilde{\theta}^B(f(Q))$$

Arithmetic on theta coordinates

Addition Formula

$$\mathcal{H}\left(\theta^A(P+Q)\odot\theta^A(P-Q)\right)\odot\mathcal{H}\left(\theta^A(0)^{\odot 2}\right)=\left(\widetilde{\theta}^B(f(P))\odot\widetilde{\theta}^B(f(Q))\right)\odot\left(\widetilde{\theta}^B(0)^{\odot 2}\right)$$

Arithmetic on theta coordinates

Addition Formula

$$\mathcal{H}\left(\theta^A(P+Q)\odot\theta^A(P-Q)\right)\odot\mathcal{H}\left(\theta^A(0)^{\odot 2}\right)=\left(\widetilde{\theta}^B(f(P))\odot\widetilde{\theta}^B(f(Q))\right)\odot\left(\widetilde{\theta}^B(0)^{\odot 2}\right)$$

$$=\left(\widetilde{\theta}^B(f(P))\odot\widetilde{\theta}^B(0)\right)\odot\left(\widetilde{\theta}^B(f(Q))\odot\widetilde{\theta}^B(0)\right)=\mathcal{H}\left(\theta^A(P)^{\odot 2}\right)\cdot\mathcal{H}\left(\theta^A(Q)^{\odot 2}\right)$$

Arithmetic on theta coordinates

Addition Formula

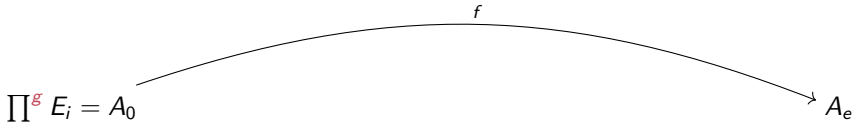
$$\mathcal{H}\left(\theta^A(P+Q)\odot\theta^A(P-Q)\right)\odot\mathcal{H}\left(\theta^A(0)^{\odot 2}\right)=\left(\widetilde{\theta}^B(f(P))\odot\widetilde{\theta}^B(f(Q))\right)\odot\left(\widetilde{\theta}^B(0)^{\odot 2}\right)$$

$$=\left(\widetilde{\theta}^B(f(P))\odot\widetilde{\theta}^B(0)\right)\odot\left(\widetilde{\theta}^B(f(Q))\odot\widetilde{\theta}^B(0)\right)=\mathcal{H}\left(\theta^A(P)^{\odot 2}\right)\cdot\mathcal{H}\left(\theta^A(Q)^{\odot 2}\right)$$

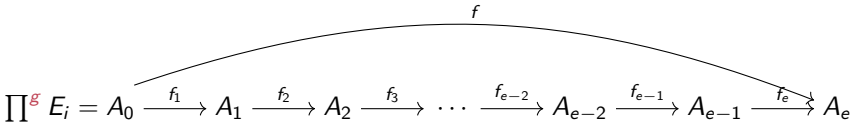
- [Gau07] This is a differential arithmetic on A.
  - simple !
  - fast !

Table of Contents

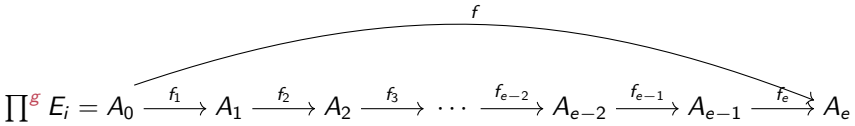
Computing Isogenies



Computing Isogenies

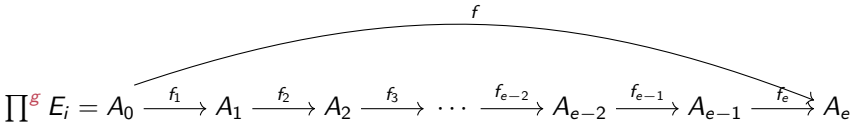


Computing Isogenies



- Building block: $\theta^A(P) \xrightarrow{f} \theta^B(f(P))$:

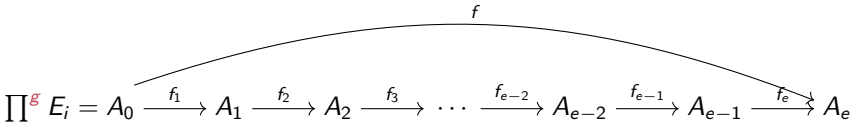
Computing Isogenies



- Building block: $\theta^A(P) \xrightarrow{f} \theta^B(f(P))$:

$$\theta^A(P) \xrightarrow{S} \theta^A(P)^{\odot 2} \xrightarrow{\mathcal{H}} \mathcal{H}(\theta^A(P)^{\odot 2}) \xrightarrow{\odot \widetilde{\theta}^B(0_B)^{\odot -1}} \widetilde{\theta}^B(f(P)) \xrightarrow{\mathcal{H}} \theta^B(f(P)).$$

Computing Isogenies



- Building block: $\theta^A(P) \xrightarrow{f} \theta^B(f(P))$:

$$\theta^A(P) \xrightarrow{S} \theta^A(P)^{\odot 2} \xrightarrow{\mathcal{H}} \mathcal{H}(\theta^A(P)^{\odot 2}) \xrightarrow{\odot \widetilde{\theta}^B(0_B)^{\odot -1}} \widetilde{\theta}^B(f(P)) \xrightarrow{\mathcal{H}} \theta^B(f(P)).$$

- Bottleneck: How do we compute $\widetilde{\theta}^B(0_B)^{\odot -1}$?
  - Not trivial !

Computing the inverse dual theta null point

$$\widetilde{\theta}^B(0)^{\odot -1} \quad \rightsquigarrow \quad \theta^B(0)$$

Computing the inverse dual theta null point

$$A[8] = \langle S_1, \cdots, S_g, T_1, \cdots, T_g \rangle$$

$$A[4] = [2](K_S \oplus K_T) \xrightarrow{\ker(f)=[4]K_T} B[4] = [2]f(K_S) \oplus f(K_T)$$

$$\Downarrow \qquad\qquad \Downarrow$$

$$\Theta^A \qquad\qquad \Theta^B$$

Computing the inverse dual theta null point

$$A[8] = \langle S_1, \cdots, S_g, T_1, \cdots, T_g \rangle$$

$$A[4] = [2](K_S \oplus K_T) \xrightarrow{\ker(f)=[4]K_T} B[4] = [2]f(K_S) \oplus f(K_T)$$

$$\Downarrow \qquad\qquad\qquad\qquad \Downarrow$$

$$\Theta^A \qquad\qquad\qquad\qquad \Theta^B$$

$$\forall \mathbf{k} \in \mathbb{Z}_2^g,\ T_{\mathbf{k}} = \sum_{i=1}^{g} [k_i] T_i, \quad \overbrace{\mathcal{H}\left(\theta^A(T_{\mathbf{k}})^{\odot 2}\right)}^{\textit{computable}} = \widetilde{\theta}^B(f(T_{\mathbf{k}})) \odot \widetilde{\theta}^B(0)$$

Computing the inverse dual theta null point

$$A[8] = \langle S_1, \cdots, S_g, T_1, \cdots, T_g \rangle$$

$$A[4] = [2](K_S \oplus K_T) \xrightarrow{\ker(f)=[4]K_T} B[4] = [2]f(K_S) \oplus f(K_T)$$

$$\Downarrow \qquad\qquad\qquad\qquad \Downarrow$$

$$\Theta^A \qquad\qquad\qquad\qquad \Theta^B$$

$$\forall \mathbf{k} \in \mathbb{Z}_2^g,\ T_{\mathbf{k}} = \sum_{i=1}^{g} [k_i] T_i, \quad \overbrace{\mathcal{H}\left(\theta^A(T_{\mathbf{k}})^{\odot 2}\right)}^{\textit{computable}} = \widetilde{\theta}^B(f(T_{\mathbf{k}})) \odot \widetilde{\theta}^B(0)$$

$$\widetilde{\theta}^B(f(T_{\mathbf{k}})) \text{ is 1-eigenvector of } \mathfrak{g}_{S_{\mathbf{k}}} \implies \widetilde{\theta}^B_j(f(T_{\mathbf{k}})) = \widetilde{\theta}^B_{j+\mathbf{k}}(f(T_{\mathbf{k}}))$$

Computing the inverse dual theta null point

$$A[8] = \langle S_1, \cdots, S_g, T_1, \cdots, T_g \rangle$$

$$A[4] = [2](K_S \oplus K_T) \xrightarrow{\ker(f)=[4]K_T} B[4] = [2]f(K_S) \oplus f(K_T)$$

$$\Downarrow \qquad\qquad\qquad\qquad \Downarrow$$

$$\Theta^A \qquad\qquad\qquad\qquad \Theta^B$$

$$\forall \mathbf{k} \in \mathbb{Z}_2^g,\ T_{\mathbf{k}} = \sum_{i=1}^{g} [k_i] T_i, \quad \overbrace{\mathcal{H}\left(\theta^A(T_{\mathbf{k}})^{\odot 2}\right)}^{\textit{computable}} = \widetilde{\theta}^B(f(T_{\mathbf{k}})) \odot \widetilde{\theta}^B(0)$$

$$\widetilde{\theta}^B(f(T_{\mathbf{k}})) \text{ is 1-eigenvector of } \mathfrak{g}_{S_{\mathbf{k}}} \implies \widetilde{\theta}^B_j(f(T_{\mathbf{k}})) = \widetilde{\theta}^B_{j+\mathbf{k}}(f(T_{\mathbf{k}}))$$

Goal: [DMPR24, Dar24] Solve the equation systems

$$\left\{ \widetilde{\theta}^B_i(f(T_{\mathbf{k}})) \cdot \widetilde{\theta}^B_i(0) = \alpha_{i,\mathbf{k}} \,\middle|\, \mathbf{k} \in S \subseteq \mathbb{Z}_2^g, i \in [2^g] \right\}$$

IIP

Let:

- $S \subseteq \mathbb{Z}_2^g$ be the *support*.
- $(\pi_{i,j})_{i \in \mathbb{Z}_2^g, j \in S}$ be such:

$$\forall i \in \mathbb{Z}_2^g, j \in S, \pi_{i,j} := \widetilde{\theta}_i^B(0) \cdot \widetilde{\theta}_i^B(f(T_j))$$

IIP

Let:

- $S \subseteq \mathbb{Z}_2^g$ be the *support*.
- $(\pi_{i,j})_{i \in \mathbb{Z}_2^g, j \in S}$ be such:

$$\forall i \in \mathbb{Z}_2^g, j \in S, \pi_{i,j} := \widetilde{\theta}_i^B(0) \cdot \widetilde{\theta}_i^B(f(T_j))$$

Inverse Interpolation Problem

$$(\pi_{i,j})_{i \in \mathbb{Z}_2^g, j \in S} \xrightarrow{Compute^a} \mathbf{x}^{\odot -1} := (x_i^{-1})_{i \in \mathbb{Z}_2^g}$$

$$\text{such that } \forall i \in \mathbb{Z}_2^g, j \in S, \quad x_i^{-1} \cdot \pi_{i,j} = x_{i+j}^{-1} \cdot \pi_{i+j,j},$$

a: up to projective factor

IIP

Let:

- $S \subseteq \mathbb{Z}_2^g$ be the *support*.
- $(\pi_{i,j})_{i \in \mathbb{Z}_2^g, j \in S}$ be such:

$$\forall i \in \mathbb{Z}_2^g, j \in S, \pi_{i,j} := \widetilde{\theta}_i^B(0) \cdot \widetilde{\theta}_i^B(f(T_j))$$

Inverse Interpolation Problem

$$(\pi_{i,j})_{i \in \mathbb{Z}_2^g, j \in S} \xrightarrow{Compute^a} \mathbf{x}^{\odot -1} := (x_i^{-1})_{i \in \mathbb{Z}_2^g}$$

$$\text{such that } \forall i \in \mathbb{Z}_2^g, j \in S, \quad x_i^{-1} \cdot \pi_{i,j} = x_{i+j}^{-1} \cdot \pi_{i+j,j},$$

a: up to projective factor

[DD26] IIP theorem (informal)

It's just graph topology !

HIIP

Let:

- $S \subseteq \mathbb{Z}_2^g$ be the *support*.
- $(\pi_{i,j})_{i \in \mathbb{Z}_2^g, j \in S}$ be such:

$$\forall i \in \mathbb{Z}_2^g, j \in S, \pi_{i,j} := \widetilde{\theta}_i^B(0) \cdot \widetilde{\theta}_i^B(f(T_j))$$

Hypercube Inverse Interpolation Problem

$$(\pi_{i,j})_{i \in \mathbb{Z}_2^g, j \in S} \xrightarrow{Compute^a} \mathbf{x}^{\odot -1} := (x_i^{-1})_{i \in \mathbb{Z}_2^g}$$

$$\text{such that } \forall i \in \mathbb{Z}_2^g, j \in S, \quad x_i^{-1} \cdot \pi_{i,j} = x_{i+j}^{-1} \cdot \pi_{i+j,j},$$

a: up to projective factor

[DD26] HIIP theorem (informal)

It's just graph topology !

HIIP as Graph Theory

$\pi_{i,j} \leftrightsquigarrow G := (V, E)$ codomain graph

- x_i are vertices.

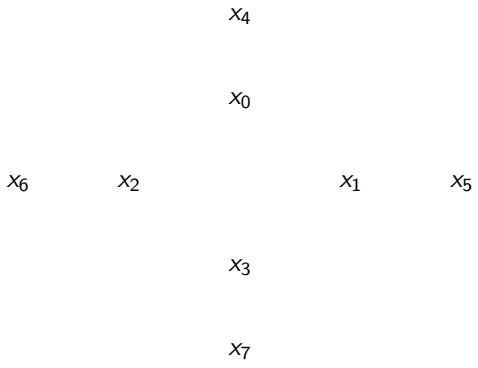


Figure: Codomain Graph G for $g = 3$, $S = \{\quad\}$

[1] assuming $\pi_{i,i+k}, \pi_{i,i+k} \neq 0$

HIIP as Graph Theory

$\pi_{i,j} \leftrightsquigarrow G := (V, E)$ codomain graph

- x_i are vertices.
- $\{x_i, x_k\} \in E \overset{1}{\iff} i + k \in S$

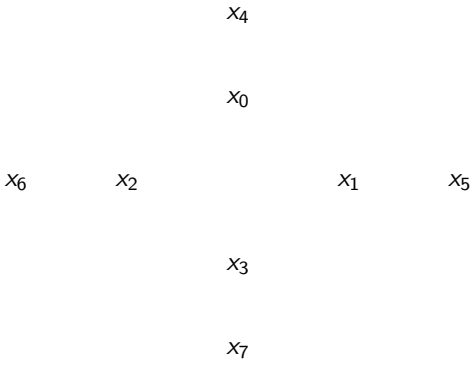


Figure: Codomain Graph G for $g = 3$, $S = \{\quad\}$

[1] assuming $\pi_{i,i+k}, \pi_{i,i+k} \neq 0$

HIIP as Graph Theory

$\pi_{i,j} \leftrightsquigarrow G := (V, E)$ codomain graph

- x_i are vertices.
- $\{x_i, x_k\} \in E \overset{1}{\iff} i + k \in S$

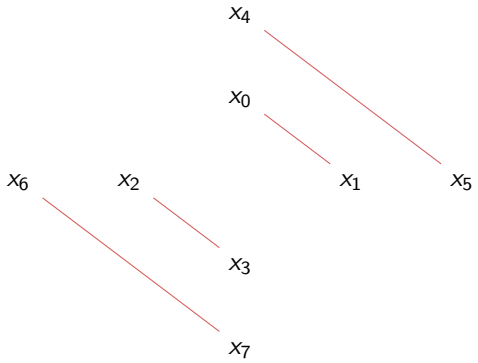


Figure: Codomain Graph G for $g = 3$, $S = \{1 \quad \}$

[1] assuming $\pi_{i,i+k}, \pi_{i,i+k} \neq 0$

HIIP as Graph Theory

$\pi_{i,j} \leftrightsquigarrow G := (V, E)$ codomain graph

- x_i are vertices.
- $\{x_i, x_k\} \in E \overset{1}{\iff} i + k \in S$

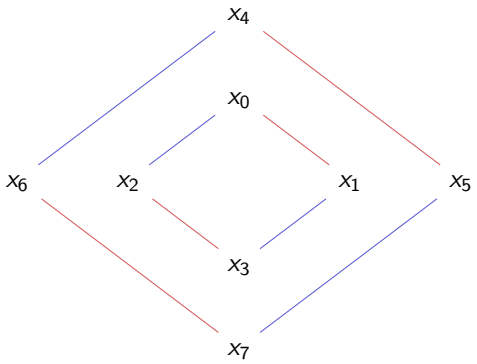


Figure: Codomain Graph G for $g = 3$, $S = \{1, 2 \quad \}$

[1] assuming $\pi_{i,i+k}, \pi_{i,i+k} \neq 0$

HIIP as Graph Theory

$\pi_{i,j} \leftrightsquigarrow G := (V, E)$ codomain graph

- x_i are vertices.
- $\{x_i, x_k\} \in E \overset{1}{\iff} i + k \in S$

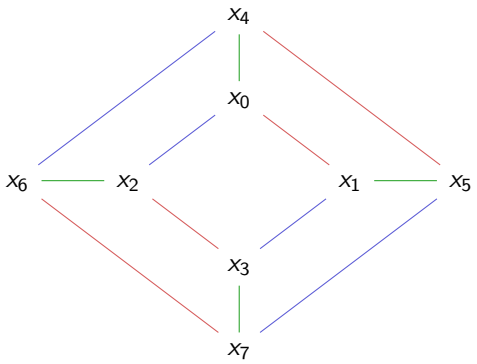


Figure: Codomain Graph G for $g = 3$, $S = \{1, 2, 4\}$

[1] assuming $\pi_{i,i+k}, \pi_{i,i+k} \neq 0$

HIIP as Graph Theory

$\pi_{i,j} \leftrightsquigarrow G := (V, E)$ codomain graph

- x_i are vertices.
- $\{x_i, x_k\} \in E \overset{1}{\iff} i + k \in S$

HIIP Theorem I

HIIP has a unique solution

$\iff$ G is connected

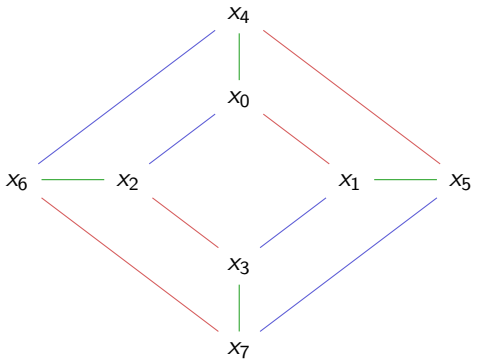


Figure: Codomain Graph G for $g = 3$, $S = \{1, 2, 4\}$

[1] assuming $\pi_{i,i+k}, \pi_{i,i+k} \neq 0$

HIIP as Graph Theory

$\pi_{i,j} \leftrightsquigarrow G := (V, E)$ codomain graph

- x_i are vertices.
- $\{x_i, x_k\} \in E \overset{1}{\iff} i + k \in S$

HIIP Theorem I

HIIP has a unique solution

$\iff$ G is connected

- We know when the codomain is computable !

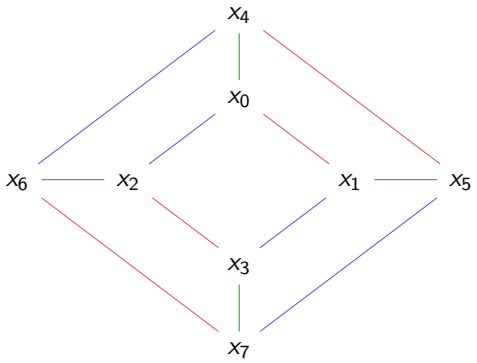
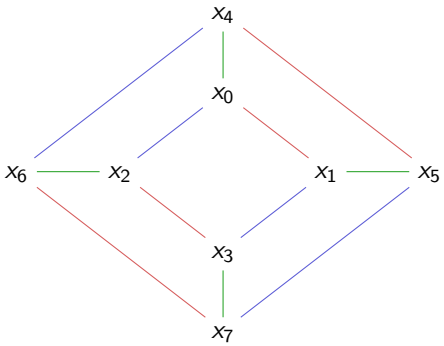


Figure: Codomain Graph G for $g = 3$, $S = \{1, 2, 4\}$

[1] assuming $\pi_{i,i+k}, \pi_{i,i+k} \neq 0$

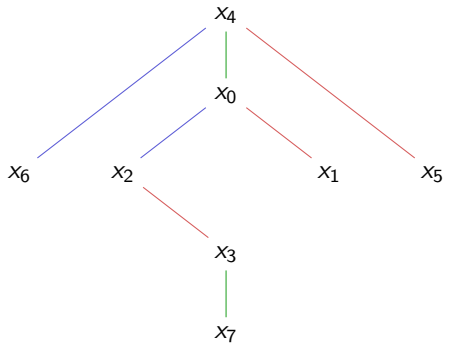
Formulae from graph theory

Let $\mathcal{T}$ be a spanning tree of G.



Formulae from graph theory

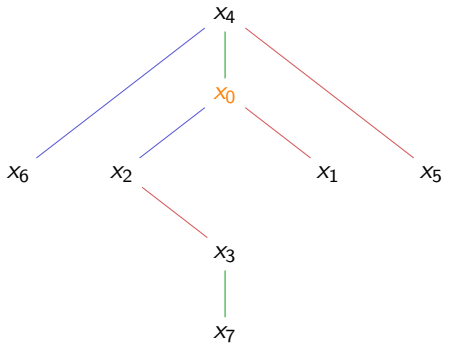
Let $\mathcal{T}$ be a spanning tree of G.



Formulae from graph theory

Let $\mathcal{T}$ be a spanning tree of G.

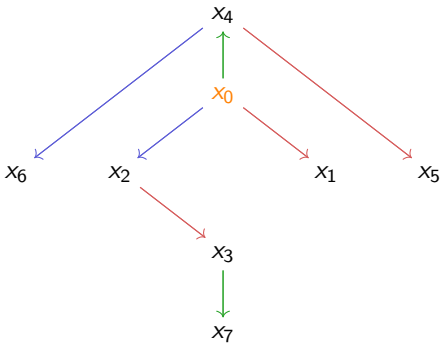
$$\forall i \in \mathbb{Z}_2^g, \text{ set } \delta_i : (\mathbb{Z}_2)^g \backslash \{i\} \xrightarrow{\sim} E_{\mathcal{T}}$$



Formulae from graph theory

Let $\mathcal{T}$ be a spanning tree of G.

$$\forall i \in \mathbb{Z}_2^g, \text{ set } \delta_i : (\mathbb{Z}_2)^g \backslash \{i\} \xrightarrow{\sim} E_{\mathcal{T}}$$

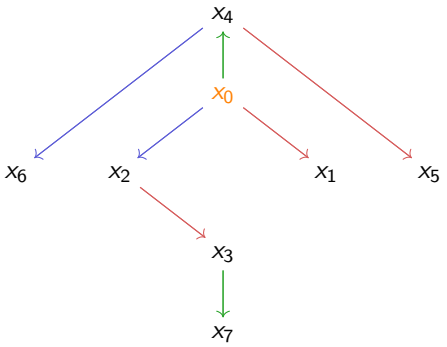


Formulae from graph theory

Let $\mathcal{T}$ be a spanning tree of G.

$$\forall i \in \mathbb{Z}_2^g, \text{ set } \delta_i : (\mathbb{Z}_2)^g \backslash \{i\} \xrightarrow{\sim} E_{\mathcal{T}}$$

$$x_i^{-1} := \prod_{k \neq i} \pi_{k, j_{\delta_i(k)}} = \prod_{k \neq i} \Big(U_k(0) \cdot U_k\big(f(T_{j_{\delta_i(k)}})\big) \Big)$$



Formulae from graph theory

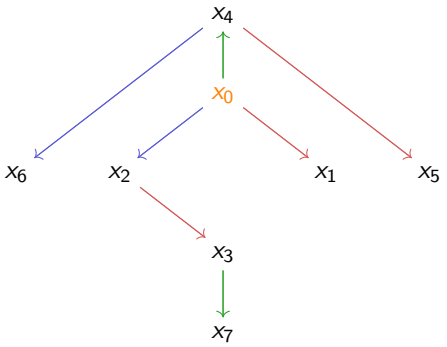
Let $\mathcal{T}$ be a spanning tree of G.

$$\forall i \in \mathbb{Z}_2^g, \text{ set } \delta_i : (\mathbb{Z}_2)^g \backslash \{i\} \xrightarrow{\sim} E_{\mathcal{T}}$$

$$x_i^{-1} := \prod_{k \neq i} \pi_{k, j_{\delta_i(k)}} = \prod_{k \neq i} \Big(U_k(0) \cdot U_k\big(f(T_{j_{\delta_i(k)}})\big) \Big)$$

HIIP Theorem II

It is a valid solution HIIP !



Formulae from graph theory

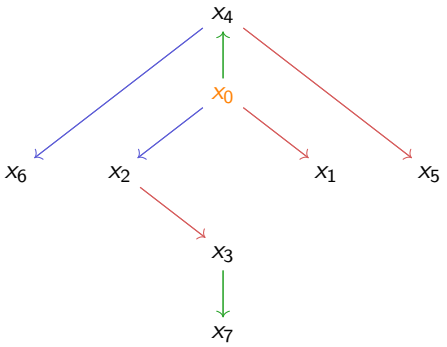
Let $\mathcal{T}$ be a spanning tree of G.

$$\forall i \in \mathbb{Z}_2^g, \text{ set } \delta_i : (\mathbb{Z}_2)^g \backslash \{i\} \xrightarrow{\sim} E_{\mathcal{T}}$$

$$x_i^{-1} := \prod_{k \neq i} \pi_{k, j_{\delta_i(k)}} = \prod_{k \neq i} \Big(U_k(0) \cdot U_k\big(f(T_{j_{\delta_i(k)}})\big) \Big)$$

HIIP Theorem II

It is a valid solution HIIP !



Formulae from graph theory

Let $\mathcal{T}$ be a spanning tree of G.

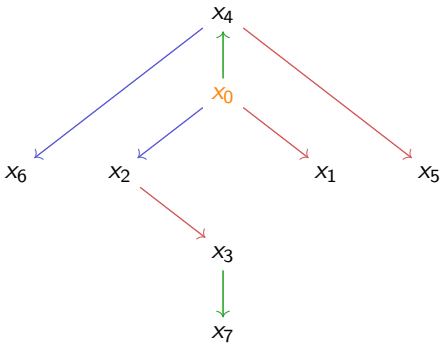
$$\forall i \in \mathbb{Z}_2^g, \text{ set } \delta_i : (\mathbb{Z}_2)^g \backslash \{i\} \xrightarrow{\sim} E_{\mathcal{T}}$$

$$x_i^{-1} := \prod_{k \neq i} \pi_{k, j_{\delta_i(k)}} = \prod_{k \neq i} \Big(U_k(0) \cdot U_k\big(f(T_{j_{\delta_i(k)}})\big) \Big)$$

HIIP Theorem II

It is a valid solution HIIP !

- Need good spanning tree of Hypercubes.



The case for Hamiltonian paths

- Introducing: $\mathcal{G}$ Gray paths on Hypercubes H_g.

$$\eta : [2^g] \xrightarrow{\cong} \mathcal{G}$$

$$\eta(i) := i \oplus (i \gg 1)$$

The case for Hamiltonian paths

- Introducing: $\mathcal{G}$ Gray paths on Hypercubes H_g.

$$\eta : [2^g] \xrightarrow{\cong} \mathcal{G}$$

$$\eta(i) := i \oplus (i \gg 1)$$

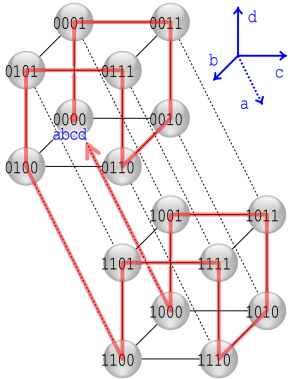


Figure: Gray code in a Tesseract

The case for Hamiltonian paths

- Introducing: $\mathcal{G}$ Gray paths on Hypercubes H_g.

$$\eta : [2^g] \xrightarrow{\cong} \mathcal{G}$$

$$\eta(i) := i \oplus (i \gg 1)$$

$$x_{\eta(i)}^{-1} = \left(\prod_{j=0}^{i-1} \pi_{\eta(j),s_j} \right) \cdot \left(\prod_{j=i}^{2^g-2} \pi_{\eta(j+1),s_j} \right)$$

with $s_i := \eta(i+1) - \eta(i)$.

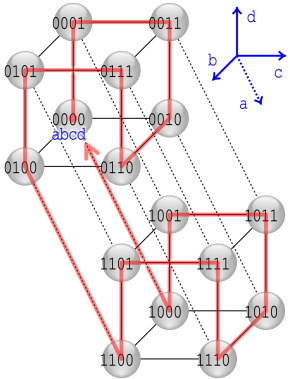


Figure: Gray code in a Tesseract

Codomain computation in its full glory

$$\begin{pmatrix}
\pi_{\eta(1),s_0} & \pi_{\eta(2),s_1} & \cdots & \pi_{\eta(2^{g-1}-1),s_{2^{g-1}-2}} & \pi_{\eta(2^{g-1}),s_{2^{g-1}-1}} & \cdots & \pi_{\eta(2^g-2),s_{2^g-3}} & \pi_{\eta(2^g-1),s_{2^g-2}} \\
\pi_{\eta(0),s_0} & \pi_{\eta(2),s_1} & \cdots & \pi_{\eta(2^{g-1}-1),s_{2^{g-1}-2}} & \pi_{\eta(2^{g-1}),s_{2^{g-1}-1}} & \cdots & \pi_{\eta(2^g-2),s_{2^g-3}} & \pi_{\eta(2^g-1),s_{2^g-2}} \\
\vdots & & \ddots & \vdots & \vdots & & \vdots & \vdots \\
\pi_{\eta(0),s_0} & \pi_{\eta(1),s_1} & \cdots & \pi_{\eta(2^{g-1}-1),s_{2^{g-1}-2}} & \pi_{\eta(2^{g-1}),s_{2^{g-1}-1}} & \cdots & \pi_{\eta(2^g-2),s_{2^g-3}} & \pi_{\eta(2^g-1),s_{2^g-2}} \\
\pi_{\eta(0),s_0} & \pi_{\eta(1),s_1} & \cdots & \pi_{\eta(2^{g-1}-2),s_{2^{g-1}-2}} & \pi_{\eta(2^{g-1}),s_{2^{g-1}-1}} & \cdots & \pi_{\eta(2^g-2),s_{2^g-3}} & \pi_{\eta(2^g-1),s_{2^g-2}} \\
\pi_{\eta(0),s_0} & \pi_{\eta(1),s_1} & \cdots & \pi_{\eta(2^{g-1}-2),s_{2^{g-1}-2}} & \pi_{\eta(2^{g-1}-1),s_{2^{g-1}-1}} & \cdots & \pi_{\eta(2^g-2),s_{2^g-3}} & \pi_{\eta(2^g-1),s_{2^g-2}} \\
\vdots & \vdots & & \vdots & \vdots & \ddots & & \vdots \\
\pi_{\eta(0),s_0} & \pi_{\eta(1),s_1} & \cdots & \pi_{\eta(2^{g-1}-2),s_{2^{g-1}-2}} & \pi_{\eta(2^{g-1}-1),s_{2^{g-1}-1}} & \cdots & \pi_{\eta(2^g-3),s_{2^g-3}} & \pi_{\eta(2^g-1),s_{2^g-2}} \\
\pi_{\eta(0),s_0} & \pi_{\eta(1),s_1} & \cdots & \pi_{\eta(2^{g-1}-2),s_{2^{g-1}-2}} & \pi_{\eta(2^{g-1}-1),s_{2^{g-1}-1}} & \cdots & \pi_{\eta(2^g-3),s_{2^g-3}} & \pi_{\eta(2^g-2),s_{2^g-2}}
\end{pmatrix}$$

Figure: Structure of the products in an Hamiltonian path

Codomain computation in its full glory

$$\begin{pmatrix}
\pi_{\eta(1),s_0} & \pi_{\eta(2),s_1} & \cdots & \pi_{\eta(2^{g-1}-1),s_{2^{g-1}-2}} & \pi_{\eta(2^{g-1}),s_{2^{g-1}-1}} & \cdots & \pi_{\eta(2^g-2),s_{2^g-3}} & \pi_{\eta(2^g-1),s_{2^g-2}} \\
\pi_{\eta(0),s_0} & \pi_{\eta(2),s_1} & \cdots & \pi_{\eta(2^{g-1}-1),s_{2^{g-1}-2}} & \pi_{\eta(2^{g-1}),s_{2^{g-1}-1}} & \cdots & \pi_{\eta(2^g-2),s_{2^g-3}} & \pi_{\eta(2^g-1),s_{2^g-2}} \\
\vdots & & \ddots & \vdots & \vdots & & \vdots & \vdots \\
\pi_{\eta(0),s_0} & \pi_{\eta(1),s_1} & \cdots & \pi_{\eta(2^{g-1}-1),s_{2^{g-1}-2}} & \pi_{\eta(2^{g-1}),s_{2^{g-1}-1}} & \cdots & \pi_{\eta(2^g-2),s_{2^g-3}} & \pi_{\eta(2^g-1),s_{2^g-2}} \\
\pi_{\eta(0),s_0} & \pi_{\eta(1),s_1} & \cdots & \pi_{\eta(2^{g-1}-2),s_{2^{g-1}-2}} & \pi_{\eta(2^{g-1}),s_{2^{g-1}-1}} & \cdots & \pi_{\eta(2^g-2),s_{2^g-3}} & \pi_{\eta(2^g-1),s_{2^g-2}} \\
\pi_{\eta(0),s_0} & \pi_{\eta(1),s_1} & \cdots & \pi_{\eta(2^{g-1}-2),s_{2^{g-1}-2}} & \pi_{\eta(2^{g-1}-1),s_{2^{g-1}-1}} & \cdots & \pi_{\eta(2^g-2),s_{2^g-3}} & \pi_{\eta(2^g-1),s_{2^g-2}} \\
\vdots & \vdots & & \vdots & \vdots & \ddots & & \vdots \\
\pi_{\eta(0),s_0} & \pi_{\eta(1),s_1} & \cdots & \pi_{\eta(2^{g-1}-2),s_{2^{g-1}-2}} & \pi_{\eta(2^{g-1}-1),s_{2^{g-1}-1}} & \cdots & \pi_{\eta(2^g-3),s_{2^g-3}} & \pi_{\eta(2^g-1),s_{2^g-2}} \\
\pi_{\eta(0),s_0} & \pi_{\eta(1),s_1} & \cdots & \pi_{\eta(2^{g-1}-2),s_{2^{g-1}-2}} & \pi_{\eta(2^{g-1}-1),s_{2^{g-1}-1}} & \cdots & \pi_{\eta(2^g-3),s_{2^g-3}} & \pi_{\eta(2^g-2),s_{2^g-2}}
\end{pmatrix}$$

Figure: Structure of the products in an Hamiltonian path

- Computing HIIP can be done in $(3 \cdot 2^g - 6)\mathbf{M}$!

Codomain computation in its full glory

$$\begin{pmatrix}
\pi_{\eta(1),s_0} & \pi_{\eta(2),s_1} & \cdots & \pi_{\eta(2^{g-1}-1),s_{2^{g-1}-2}} & \pi_{\eta(2^{g-1}),s_{2^{g-1}-1}} & \cdots & \pi_{\eta(2^g-2),s_{2^g-3}} & \pi_{\eta(2^g-1),s_{2^g-2}} \\
\pi_{\eta(0),s_0} & \pi_{\eta(2),s_1} & \cdots & \pi_{\eta(2^{g-1}-1),s_{2^{g-1}-2}} & \pi_{\eta(2^{g-1}),s_{2^{g-1}-1}} & \cdots & \pi_{\eta(2^g-2),s_{2^g-3}} & \pi_{\eta(2^g-1),s_{2^g-2}} \\
\vdots & & \ddots & \vdots & \vdots & & \vdots & \vdots \\
\pi_{\eta(0),s_0} & \pi_{\eta(1),s_1} & \cdots & \pi_{\eta(2^{g-1}-1),s_{2^{g-1}-2}} & \pi_{\eta(2^{g-1}),s_{2^{g-1}-1}} & \cdots & \pi_{\eta(2^g-2),s_{2^g-3}} & \pi_{\eta(2^g-1),s_{2^g-2}} \\
\pi_{\eta(0),s_0} & \pi_{\eta(1),s_1} & \cdots & \pi_{\eta(2^{g-1}-2),s_{2^{g-1}-2}} & \pi_{\eta(2^{g-1}),s_{2^{g-1}-1}} & \cdots & \pi_{\eta(2^g-2),s_{2^g-3}} & \pi_{\eta(2^g-1),s_{2^g-2}} \\
\pi_{\eta(0),s_0} & \pi_{\eta(1),s_1} & \cdots & \pi_{\eta(2^{g-1}-2),s_{2^{g-1}-2}} & \pi_{\eta(2^{g-1}-1),s_{2^{g-1}-1}} & \cdots & \pi_{\eta(2^g-2),s_{2^g-3}} & \pi_{\eta(2^g-1),s_{2^g-2}} \\
\vdots & \vdots & & \vdots & \vdots & \ddots & & \vdots \\
\pi_{\eta(0),s_0} & \pi_{\eta(1),s_1} & \cdots & \pi_{\eta(2^{g-1}-2),s_{2^{g-1}-2}} & \pi_{\eta(2^{g-1}-1),s_{2^{g-1}-1}} & \cdots & \pi_{\eta(2^g-3),s_{2^g-3}} & \pi_{\eta(2^g-1),s_{2^g-2}} \\
\pi_{\eta(0),s_0} & \pi_{\eta(1),s_1} & \cdots & \pi_{\eta(2^{g-1}-2),s_{2^{g-1}-2}} & \pi_{\eta(2^{g-1}-1),s_{2^{g-1}-1}} & \cdots & \pi_{\eta(2^g-3),s_{2^g-3}} & \pi_{\eta(2^g-2),s_{2^g-2}}
\end{pmatrix}$$

Figure: Structure of the products in an Hamiltonian path

- Computing HIIP can be done in $(3 \cdot 2^g - 6)\mathbf{M}$!
- Can be highly parallelised !

Retrospectively trivial

Algorithm 1: Solution to the HIIP

Data: HIIP input data, including a subset $S \subseteq (\mathbb{Z}/2\mathbb{Z})^g$, a graph $G := ((\mathbb{Z}/2\mathbb{Z})^g, E)$ and matrix $(\pi_{\mathbf{i},\mathbf{j}})_{\mathbf{i}\in(\mathbb{Z}/2\mathbb{Z})^g,\mathbf{j}\in S}$. A Hamiltonian path $\eta : [\![0, 2^g - 1]\!] \xrightarrow{\sim} (\mathbb{Z}/2\mathbb{Z})^g$ in G.

Result: A solution $(x_{\eta(i)}^{\odot -1})_{0\leq i\leq 2^g-1}$ to the HIIP defined by the input data (up to reordering by η).

$\rho_L(0) \leftarrow 1$;
$\rho_L(1) \leftarrow \pi_{\eta(1),\mathbf{s}_1}$;
$\rho_R(2^g - 1) \leftarrow 1$;
$\rho_R(2^g - 2) \leftarrow \pi_{\eta(2^g-1),\mathbf{s}_{2^g-2}}$;
for $i \in [\![2, 2^g - 1]\!]$ **do**
  $\rho_L(i) \leftarrow \rho_L(i-1) \cdot \pi_{\eta(i),\mathbf{s}_i}$;
  $\rho_R(2^g - 1 - i) \leftarrow \rho_L(2^g - i) \cdot \pi_{\eta(2^g-i),\mathbf{s}_{2^g-1-i}}$;
end
$x_{\eta(0)}^{-1} \leftarrow \rho_R(0)$;
$x_{\eta(2^g-1)}^{-1} \leftarrow \rho_L(2^g - 1)$;
for $i \in [\![1, 2^g - 2]\!]$ **do**
  $x_{\eta(i)}^{-1} \leftarrow \rho_L(i) \cdot \rho_R(i)$;
end
return $\left(x_{\eta(i)}^{-1}\right)_{0\leq i\leq 2^g-1}$; // Total cost: $(3 \cdot 2^g - 6)\mathbf{M}$

Generic isogeny: computing cost

	dim. g	dim. 4
Old [Dar25]	$(6 \cdot 2^g - 9)\mathbf{M} + g2^g\mathbf{S} + g^2 2^g \mathbf{a}$	$87\mathbf{M} + 64\mathbf{S} + 256\mathbf{a}$
New [DD26]	$3(2^g - 2)\mathbf{M} + g2^g\mathbf{S} + g^2 2^g \mathbf{a}$	$42\mathbf{M} + 64\mathbf{S} + 256\mathbf{a}$

Generic isogeny: computing cost

	dim. g	dim. 4
Old [Dar25]	$(6 \cdot 2^g - 9)\mathbf{M} + g2^g\mathbf{S} + g^2 2^g \mathbf{a}$	$87\mathbf{M} + 64\mathbf{S} + 256\mathbf{a}$
New [DD26]	$3(2^g - 2)\mathbf{M} + g2^g\mathbf{S} + g^2 2^g \mathbf{a}$	$42\mathbf{M} + 64\mathbf{S} + 256\mathbf{a}$

Graph theory gives us formulae that are:

- Simple to implement !
- Constant time !
- *Very flexible !*

Table of Contents

Our arch nemesis: Gluing

$$\underbrace{(\overset{g}{\prod} E_i = A_0) \xrightarrow{f_1} A_1 \xrightarrow{f_2} A_2}_{\textit{Gluing}} \underbrace{\xrightarrow{f_2} \cdots \xrightarrow{f^{e-1}} A_{e-1} \xrightarrow{f_e} A_e}_{\text{generic}}$$

Our arch nemesis: Gluing

$$\underbrace{(\prod^{g} E_i = A_0) \xrightarrow{f_1} A_1 \xrightarrow{f_2} A_2}_{\textit{Gluing}} \underbrace{\xrightarrow{f_2} \cdots \xrightarrow{f^{e-1}} A_{e-1} \xrightarrow{f_e} A_e}_{\text{generic}}$$

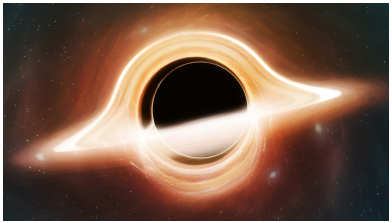


Figure: Artist view of a gluing isogeny

Our arch nemesis: Gluing

$$\underbrace{(\overset{g}{\prod} E_i = A_0) \xrightarrow{f_1} A_1 \xrightarrow{f_2} A_2}_{\textit{Gluing}} \underbrace{\xrightarrow{f_2} \cdots \xrightarrow{f^{e-1}} A_{e-1} \xrightarrow{f_e} A_e}_{\text{generic}}$$

Gluing is:

- A rabbit-hole of technicality.
- HD-chain is 90% gluing (workload).

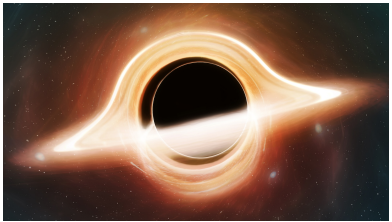


Figure: Artist view of a gluing isogeny

Our arch nemesis: Gluing

$$\underbrace{(\prod^{g} E_i = A_0) \xrightarrow{f_1} A_1 \xrightarrow{f_2} A_2}_{\textit{Gluing}} \underbrace{\xrightarrow{f_2} \cdots \xrightarrow{f^{e-1}} A_{e-1} \xrightarrow{f_e} A_e}_{\text{generic}}$$

Gluing is:

- A rabbit-hole of technicality.
- HD-chain is 90% gluing (workload).
- HIIP is black-hole compatible !

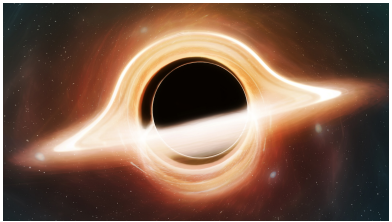


Figure: Artist view of a gluing isogeny

Dealing with zeros

Problem with gluing : $\widetilde{\theta}_i^A(0) = 0$ or $\widetilde{\theta}_i^A(f(T_j)) = 0 \implies G \subset H_g$

Dealing with zeros

Problem with gluing : $\widetilde{\theta}_i^A(0) = 0$ or $\widetilde{\theta}_i^A(f(T_j)) = 0 \implies G \subset H_g$

Case 1: $\mathcal{G} \not\subset G$

$\simeq$ a few zeros:

Dealing with zeros

Problem with gluing : $\widetilde{\theta}_i^A(0) = 0$ or $\widetilde{\theta}_i^A(f(T_j)) = 0 \implies G \subset H_g$

Case 1: $\mathcal{G} \not\subset G$

$\simeq$ a few zeros:

Figure: HD isogeny computing tool

Dealing with zeros

$$\textbf{Problem with gluing}: \widetilde{\theta}_i^A(0) = 0 \text{ or } \widetilde{\theta}_i^A(f(T_j)) = 0 \implies G \subset H_g$$

Case 1: $\mathcal{G} \not\subset G$

$\simeq$ a few zeros:

Solution: Use $\mathrm{Aut}(H_g)$:

$$\text{Find } \Delta_{\sigma,v} : i \in \mathbb{Z}_2^g \longmapsto i \circ \sigma + v$$

such that $\Delta_{\sigma,v}(\mathcal{G}) \subset G$.

Figure: HD isogeny computing tool

with $v \in \mathbb{Z}_2^g$ and $i \circ \sigma := (i_{\sigma(m)})_{1 \leq m \leq g}, \sigma \in \mathfrak{S}_g$

Dealing with zeros

Problem with gluing : $\widetilde{\theta}_i^A(0) = 0$ or $\widetilde{\theta}_i^A(f(T_j)) = 0 \implies G \subset H_g$

Case 1: $\mathcal{G} \not\subset G$

$\simeq$ a few zeros:

Solution: Use $\mathrm{Aut}(H_g)$:

$$\text{Find } \Delta_{\sigma,v} : i \in \mathbb{Z}_2^g \longmapsto i \circ \sigma + v$$

such that $\Delta_{\sigma,v}(\mathcal{G}) \subset G$.

Figure: HD isogeny computing tool

Case 2: G is not connected.

Likely working with a product variety.

with $v \in \mathbb{Z}_2^g$ and $i \circ \sigma := (i_{\sigma(m)})_{1 \leq m \leq g}, \sigma \in \mathfrak{S}_g$

Dealing with zeros

Problem with gluing : $\widetilde{\theta}_i^A(0) = 0$ or $\widetilde{\theta}_i^A(f(T_j)) = 0 \implies G \subset H_g$

Case 1: $\mathcal{G} \not\subset G$

$\simeq$ a few zeros:

Solution: Use $\mathrm{Aut}(H_g)$:

$$\text{Find } \Delta_{\sigma,v} : i \in \mathbb{Z}_2^g \longmapsto i \circ \sigma + v$$

such that $\Delta_{\sigma,v}(\mathcal{G}) \subset G$.

Figure: HD isogeny computing tool

Case 2: G is not connected.

Likely working with a product variety.

Solution: Use more points $T_k \implies$ More edges in G.

with $v \in \mathbb{Z}_2^g$ and $i \circ \sigma := (i_{\sigma(m)})_{1 \leq m \leq g}, \sigma \in \mathfrak{S}_g$

Rabbits

In qt-Pegasis, gluing graphs G are rabbits !

Rabbits

In qt-Pegasis, gluing graphs G are rabbits !

Rabbit classification lemma

Figure: Rabbit picture

Rabbits

In qt-Pegasis, gluing graphs G are rabbits !

Rabbit classification lemma

1. There are 32 rabbits, identical except for their fur colour, of which there are four.

Figure: Rabbit picture

Rabbits

In qt-Pegasis, gluing graphs G are rabbits !

Rabbit classification lemma

1. There are 32 rabbits, identical except for their fur colour, of which there are four.
2. Can dye rabbits into another colour through bit-swapping the indices.

Figure: Rabbit picture

Rabbits

In qt-Pegasis, gluing graphs G are rabbits !

Rabbit classification lemma

1. There are 32 rabbits, identical except for their fur colour, of which there are four.
2. Can dye rabbits into another colour through bit-swapping the indices.
3. Rabbits are satiated when feed 5 carrots.

Figure: Rabbit picture

Rabbits

In qt-Pegasis, gluing graphs G are rabbits !

Rabbit classification lemma

1. There are 32 rabbits, identical except for their fur colour, of which there are four.
2. Can dye rabbits into another colour through bit-swapping the indices.
3. Rabbits are satiated when feed 5 carrots.
4. Every rabbit has a skeleton that forms a Hamiltonian path in his body, with two ears on top.

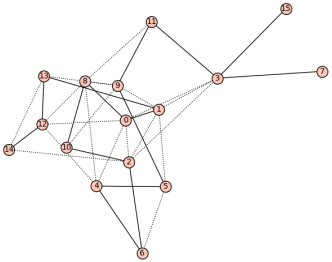


Figure: Rabbit picture

Rabbits

In qt-Pegasis, gluing graphs G are rabbits !

Rabbit classification lemma

1. There are 32 rabbits, identical except for their fur colour, of which there are four.
2. Can dye rabbits into another colour through bit-swapping the indices.
3. Rabbits are satiated when feed 5 carrots.
4. Every rabbit has a skeleton that forms a Hamiltonian path in his body, with two ears on top.

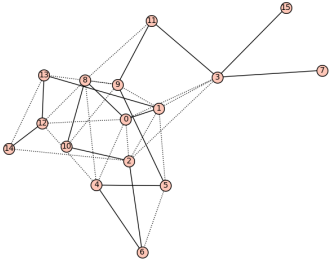


Figure: Rabbit picture

- Computing a rabbits take $(3 \cdot 2^g - 5)\mathbf{M}$
- Using other (many) technical tricks, made constant time gluing for qt-Pegasis.

Special isogenies

- For some locis of abelian varieties, $\mathrm{Aut}(A)$ big:

Special isogenies

- For some locis of abelian varieties, $\mathrm{Aut}(A)$ big:
  - 2-adherence of products (dim $2+$).
  - Fourfold of Weil-type $(2,2)$ (dim 4).

Special isogenies

- For some locis of abelian varieties, $\mathrm{Aut}(A)$ big:
  - 2-adherence of products (dim $2+$).
  - Fourfold of Weil-type $(2,2)$ (dim 4).
- Can compute their isogenies faster !

Special isogenies

- For some locis of abelian varieties, $\mathrm{Aut}(A)$ big:
  - 2-adherence of products (dim $2+$).
  - Fourfold of Weil-type $(2,2)$ (dim 4).
- Can compute their isogenies faster !

$$\sigma \in \mathrm{Aut}(A) \implies \overset{\sigma}{\sim} \text{ equivalence relation over } \theta_i^A(0)$$

Special isogenies

- For some locis of abelian varieties, $\mathrm{Aut}(A)$ big:
  - 2-adherence of products (dim $2+$).
  - Fourfold of Weil-type $(2,2)$ (dim 4).
- Can compute their isogenies faster !

$$\sigma \in \mathrm{Aut}(A) \implies \overset{\sigma}{\sim} \text{ equivalence relation over } \theta_i^A(0)$$

$$\text{Solving the HIIP over } G \iff \text{Solving the HIIP over } G_{/\overset{\sigma}{\sim}}$$

Example: Isogenies between fourfold of Weil-type $(2,2)$

We have $\iota \in \mathrm{Aut}(A), \iota^2 = -1$

Then $\theta_i^A(0) = \theta_{i\circ\sigma}^A(0)$ for $\sigma = (03)(12)$

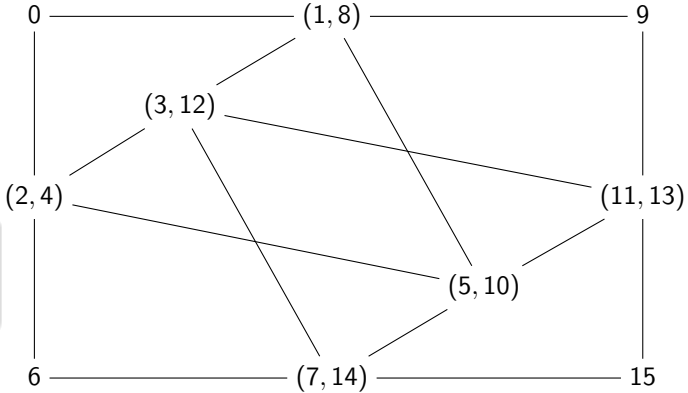
Example: Isogenies between fourfold of Weil-type $(2, 2)$

We have $\iota \in \mathrm{Aut}(A), \iota^2 = -1$

Then $\theta_i^A(0) = \theta_{i\circ\sigma}^A(0)$ for $\sigma = (03)(12)$

Weil-type $(2, 2)$ formula

- Computable using only 2 points!



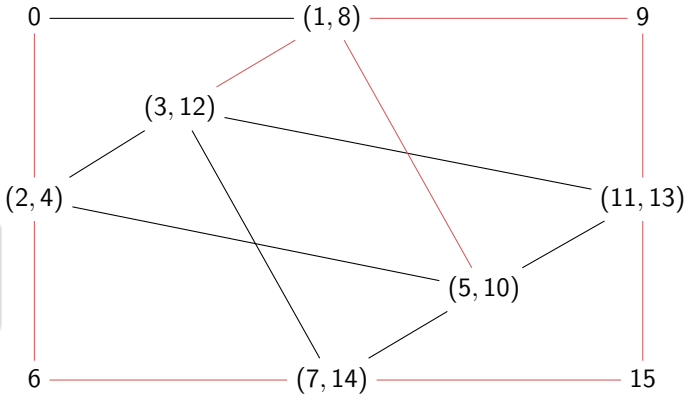
Example: Isogenies between fourfold of Weil-type $(2, 2)$

We have $\iota \in \mathrm{Aut}(A), \iota^2 = -1$

Then $\theta_i^A(0) = \theta_{i\circ\sigma}^A(0)$ for $\sigma = (03)(12)$

Weil-type $(2, 2)$ formula

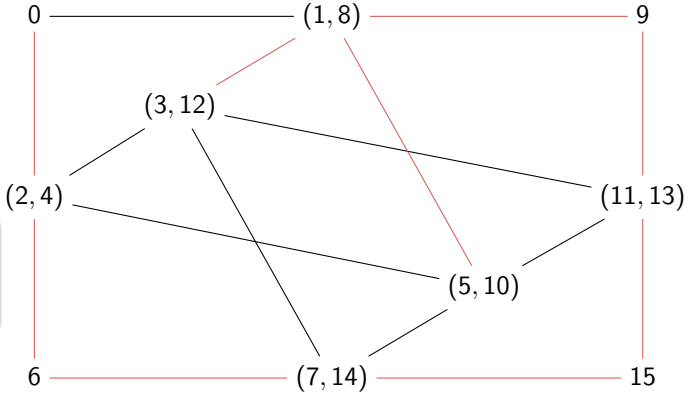
- Computable using only 2 points!
- Full of rabbits!



Example: Isogenies between fourfold of Weil-type $(2, 2)$

We have $\iota \in \mathrm{Aut}(A), \iota^2 = -1$

Then $\theta_i^A(0) = \theta_{i\circ\sigma}^A(0)$ for $\sigma = (03)(12)$



Weil-type $(2, 2)$ formula

- Computable using only 2 points!
- Full of rabbits!

Corollary

$\otimes$-MIKE is fast !

Implementation of qt-Pegasis

$\lceil \log_2(p) \rceil$	p	ARM (Mcycles)	X86 (Mcycles)	Timing (ms)
505	$27 \cdot 2^{500} - 1$	146.95	274.38	23.94
1008	$15 \cdot 2^{1004} - 1$	871.34	1627.05	146.19
1525	$5 \cdot 2^{1522} - 1$	3163.05	5208.81	543.01
2017	$5 \cdot 2^{2014} - 1$	7041.82	11192.45	1222.96
4030	$45 \cdot 2^{4024} - 1$	55228.89	83757.68	10654.93

Table: Performance of the C-implementation of 4-dimensional chain of qt-Pegasis in CPU Mcycles. Results are the average of 100 benchmark runs.

Conclusion

Isogenies are just graphs!

Conclusion

Isogenies are just graphs!

1. Dim 4 chains are constructively practical!

Conclusion

Isogenies are just graphs!

1. Dim 4 chains are constructively practical!
2. We have all the tools for generic dimension!

Conclusion

Isogenies are just graphs!

1. Dim 4 chains are constructively practical!
2. We have all the tools for generic dimension!
3. It has never been easier to join the train!

Conclusion

Isogenies are just graphs!

1. Dim 4 chains are constructively practical!
2. We have all the tools for generic dimension!
3. It has never been easier to join the train!
4. Gluing will provide you *endless* fun!

Thanks for listening !

Beware of rabbits !

Ad break

Workshop on Abelian varieties and Applications to Post-Quantum Cryptography

16 - 20 November 2026
Bernoulli center, EPFL

More info on: https://bernoulli-isogeny.github.io/index.html

Figure: EPFL (not in November)

References I

- Pierrick Dartois, *Fast computation of 2-isogenies in dimension 4 and cryptographic applications*, Cryptology ePrint Archive, Paper 2024/1180, 2024.
- Pierrick Dartois, *Fast computation of higher dimensional isogenies for cryptographic applications*, Ph.D. thesis, Université de Bordeaux, 2025.
- Pierrick Dartois and Max Duparc, *Chasing rabbits through hypercubes: Better algorithms for higher dimensional 2-isogeny computations*, Cryptology ePrint Archive, Paper 2026/114, 2026.
- Pierrick Dartois, Luciano Maino, Giacomo Pope, and Damien Robert, *An algorithmic approach to (2, 2)-isogenies in the theta model and applications to isogeny-based cryptography*, ASIACRYPT 2024, Part III (Kai-Min Chung and Yu Sasaki, eds.), LNCS, vol. 15486, Springer, Singapore, December 2024, pp. 304–338.
- Max Duparc, *Superglue: Fast formulae for (2,2)-gluing isogenies*, ASIACRYPT 2025, Part IV, LNCS, Springer, Singapore, December 2025, pp. 372–400.
- Pierrick Gaudry, *Fast genus 2 arithmetic based on theta functions*, Journal of Mathematical Cryptology **1** (2007), no. 3, 243–265.

References II


David Bryant Mumford, *On the equations defining abelian varieties. i*, Inventiones mathematicae (1966).


Adi Shamir, *Ip= pspace*, Journal of the ACM (JACM) **39** (1992), no. 4, 869–877.